

# Cyber Aces

## Module 1 – Operating Systems

### Installing Software on CentOS

By Tom Hessman, Tim Medin, Mark Baggett, Doug Burks,  
Michael Coppola, Russell Eubanks, and Ed Skoudis

Presented by Tim Medin

v15Q1

This tutorial is licensed for personal use exclusively for students and teachers to prepare for the Cyber Aces competitions. You may not use any part of it in any printed or electronic form for other purposes, nor are you allowed to redistribute it without prior written consent from the SANS Institute.

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

1

Welcome to Cyber Aces Online Module 1. In this session we will cover the ways to install software on Linux and in CentOS.

# Installing Software

- Before we install software, we must obtain it
- We can obtain it from a Linux distribution CD or from the Internet
  - Most packages are on the Internet today
- Most Linux software comes in two different forms: source or package
  - Source has to be compiled
  - Packages are generally distro-specific, but install easily

## Installing Software

Before we can install software, we must obtain the software itself. We can obtain software from a Linux distribution CD or directly from the Internet. Nowadays, most packages are retrieved from the Internet. Most Linux software downloaded from the Internet comes in two different forms: source or package. Source packages contain source code, and therefore have to be compiled. Packages are generally distro-specific, but they are much easier to install.

# Installing Software from Source (1)

- Installing from source is the traditional way to install software in the UNIX world
- This is typically done with the following commands:  
\$ **./configure**  
\$ **make**  
\$ **sudo make install**
- "configure" examines the OS environment and configures the Makefile.
- "make" uses the Makefile to compile the software.
- "make install" copies the software to the appropriate system directories

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

3

## Installing Software from Source (1)

The traditional method of software installation in the UNIX world is manually compiling source code into executable form. This is usually done with the following commands:

```
$ ./configure  
$ make  
$ sudo make install
```

The source tarball downloaded from the Internet contains a file called "configure", which we execute from the current directory by calling "./configure". This command examines the operating system and the software already installed on it and configures the Makefile which will be used in the next step. The "make" command uses the compiler that is already installed in the operating system to create binary executable programs. It references the Makefile created by the "./configure" step and compiles the source code into binary form. Finally, "make install" copies the newly-compiled binaries from the current directory to the appropriate system directories. This last step will usually copy the binaries (executables) to directories only writeable by root, as such you will need root permissions to perform this step.

## Installing Software from Source (2)

- These commands are often combined into a single command:  
# **./configure && make && make install**
  - The double ampersand is a conditional operator that says "IF the first command succeeds, THEN execute the second command"
- To remove software installed from source, enter the original source directory and run:  
# **make uninstall**
  - This will not always work

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

4

### Installing Software from Source (2)

These three commands are commonly joined together on a single line using double ampersands (&&) like this:

```
# ./configure && make && make install
```

The double ampersand is a conditional operator that says "IF the first command succeeds, THEN execute the next command".

To uninstall a program that was compiled from source, enter the original source directory and type "**make uninstall**". Unfortunately, not all software contains this feature in its Makefile.

# Package Managers

- Most Linux distros use some form of package manager to speed up the installation process and make it less error prone
  - Red Hat-based distros use RPM
  - Debian-based distros use APT
- Packages contain pre-compiled software for your distribution and processor type
- Package managers can be used from the GUI or CLI

## Package Managers

To speed up the installation process and make it less prone to errors, most modern Linux distributions use some form of package manager. Distributions based on Red Hat use RPM, the RPM Package Manager (note the recursive acronym!). Distributions based on Debian (including Ubuntu) use the DEB package format with APT. In either case, the package is a single file that contains the entire application, pre-compiled for your distribution and processor. The package can be installed using a package manager with a graphical user interface, or from the command-line.

# RPM Examples

- Use "rpm" to install RPM files:  
`# rpm -Uvh NewApplication-3.2.1.rpm`
- "rpm" can also download and install an RPM in a single step:  
`# rpm -Uvh  
http://site.example.com/NewApplication-  
3.2.1.rpm`
- To delete an application using RPM, use the "-e" option and the package name:  
`# rpm -e NewApplication`
- Most package managers can validate installed packages to make sure they haven't been tampered with. The following command can help detect tampered files on a Red Hat system:  
`# rpm -Va | sort`

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

6

## RPM Examples

To install an RPM package on a Red Hat-based system, use the "rpm" command as follows:

```
# rpm -Uvh NewApplication-3.2.1.rpm
```

The "U" means "install or upgrade", the "v" means to print more verbose information, and the "h" means to print a progress bar during the install.

Red Hat systems can download and install an RPM package in one step using a command like this:

```
# rpm -Uvh http://site.example.com/NewApplication-3.2.1.rpm
```

That same application could then be removed from the system with the following command:

```
# rpm -e NewApplication
```

If an attacker compromises a machine and modifies a file that belongs to an RPM package, then the following command can help detect that:

```
# rpm -Va | sort
```

The "V" means to verify packages, and the "a" means "all packages".

# Package Repositories

- Linux vendors maintain online repositories of all software included in their distribution
- This makes it easy to install software after installing your system, straight from the online repository
  - Rather than needing to go to a vendor's website like in the Windows world, you can get almost all software you need from one place
- Linux distros generally have tools for automating this process
  - On Red Hat systems, this tool is called "yum"

## Package Repositories

Linux vendors maintain online repositories of all of the software they've decided to include in their distribution. This means that if you did a default installation (which doesn't include every single package in the repository) and later decide that you need one of those packages, you can simply install it straight from the repo instead of having to locate it at a third-party site.

Linux distributions generally have tools for automating this process. On Red Hat systems, this tool is called "yum".

## Exercise: Package Repositories (1)



The screenshot shows a terminal window titled 'centoslive@livecd:~'. The terminal output is as follows:

```
[centoslive@livecd ~]$ nmap
bash: nmap: command not found

[centoslive@livecd ~]$ rpm -qa | grep nmap

[centoslive@livecd ~]$ yum search nmap
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: centos.arvixe.com
 * extras: centos.mirror.lstn.net
 * updates: ftp.osuosl.org

===== N/S Matched: nmap =====
nmap-frontend.noarch : The GTK+ front end for nmap
nmap.x86_64 : Network exploration tool and security scanner

Name and summary matches only, use "search all" for everything.
[centoslive@livecd ~]$
```

Yellow circles with numbers 1, 2, and 3 are placed next to the commands `nmap`, `rpm -qa | grep nmap`, and `yum search nmap` respectively. Red boxes highlight the search results for `nmap` in the `yum search` output.

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 8

### Exercise: Package Repositories (1)

1. Try to start a network scanning tool called nmap:

# **nmap**

You should receive a "command not found" error.

2. Let's verify that it's not installed by querying the RPM database:

# **rpm -qa | grep nmap**

There should be no output, verifying that the nmap RPM has not been installed.

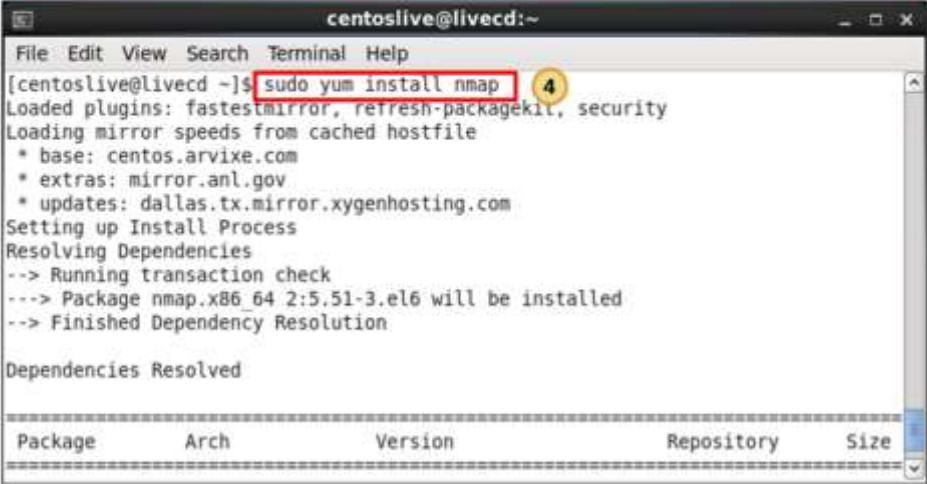
3. Use the "yum search" command to verify that the repositories have nmap:

# **yum search nmap**

Note: This requires a working internet connection



## Exercise: Package Repositories (2)



The screenshot shows a terminal window titled 'centoslive@livecd:~'. The command 'sudo yum install nmap' is entered and highlighted with a red box, with a yellow circle containing the number '4' next to it. The terminal output shows the yum command loading plugins, loading mirror speeds, setting up the install process, resolving dependencies, and running a transaction check. It indicates that the package 'nmap.x86\_64 2:5.51-3.el6' will be installed. Below the output, a table header is visible: 'Package Arch Version Repository Size'.

```
centoslive@livecd:~  
File Edit View Search Terminal Help  
[centoslive@livecd ~]$ sudo yum install nmap  
Loaded plugins: fastestmirror, refresh-packagekit, security  
Loading mirror speeds from cached hostfile  
* base: centos.arvixe.com  
* extras: mirror.anl.gov  
* updates: dallas.tx.mirror.xygenhosting.com  
Setting up Install Process  
Resolving Dependencies  
--> Running transaction check  
---> Package nmap.x86_64 2:5.51-3.el6 will be installed  
--> Finished Dependency Resolution  
  
Dependencies Resolved  
  
=====
```

Package	Arch	Version	Repository	Size
---------	------	---------	------------	------

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

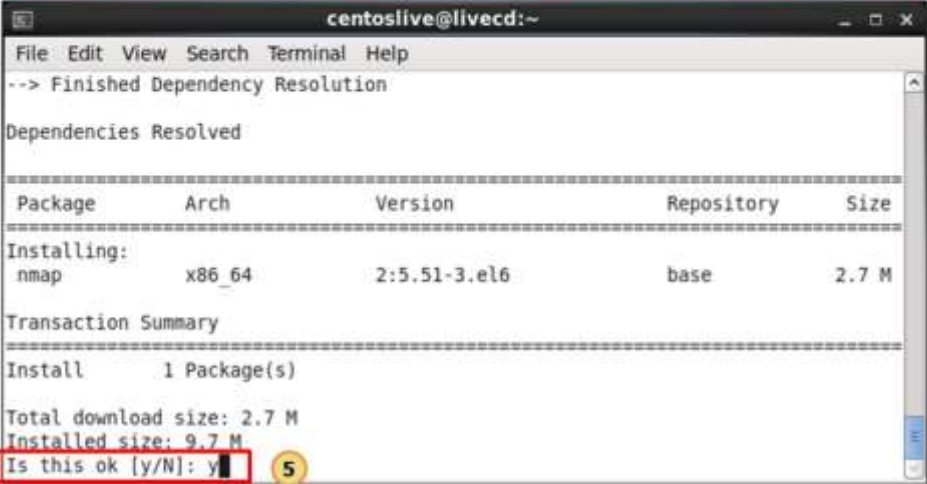
### Exercise: Package Repositories (2)

4. Use the "yum install" command to install the nmap RPM from the CentOS repositories:

\$ **sudo yum install nmap**

Note: This also requires a working internet connection

## Exercise: Package Repositories (3)



A terminal window titled 'centoslive@livecd:~' showing the output of the 'yum install nmap' command. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The output text is as follows:

```
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch           Version           Repository        Size
=====
Installing:
nmap               x86_64         2:5.51-3.el6      base              2.7 M
=====

Transaction Summary
=====
Install      1 Package(s)

Total download size: 2.7 M
Installed size: 9.7 M
Is this ok [y/N]: y
```

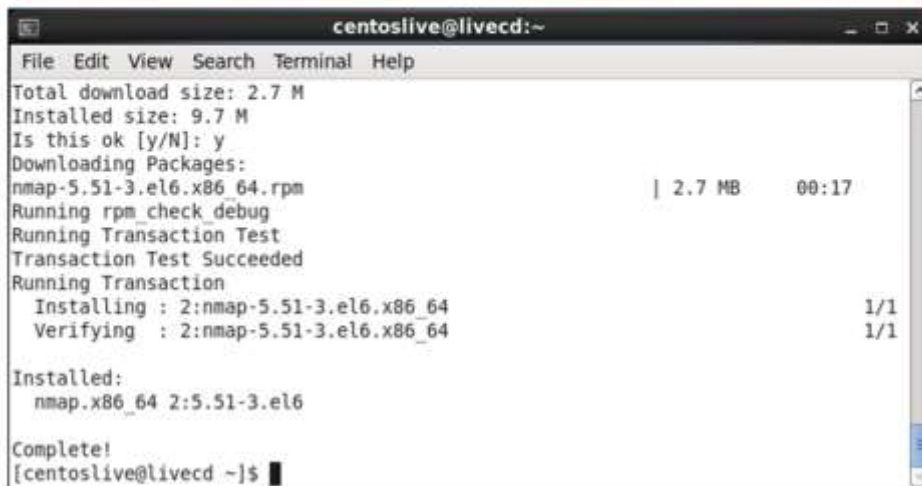
The 'Is this ok [y/N]: y' prompt is highlighted with a red rectangle. A yellow circle with the number '5' is positioned to the right of the prompt. At the bottom of the terminal window, there is a red banner with the text 'Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.' and the number '10' in the bottom right corner.

### Exercise: Package Repositories (3)

This is more of the output from the "**yum install nmap**" command on the previous slide.

5. You will be asked if this is okay before continuing; type "**y**" to continue. Note how it shows you a list of exactly what actions will be performed, including any dependencies that will be affected.

## Exercise: Package Repositories (4)

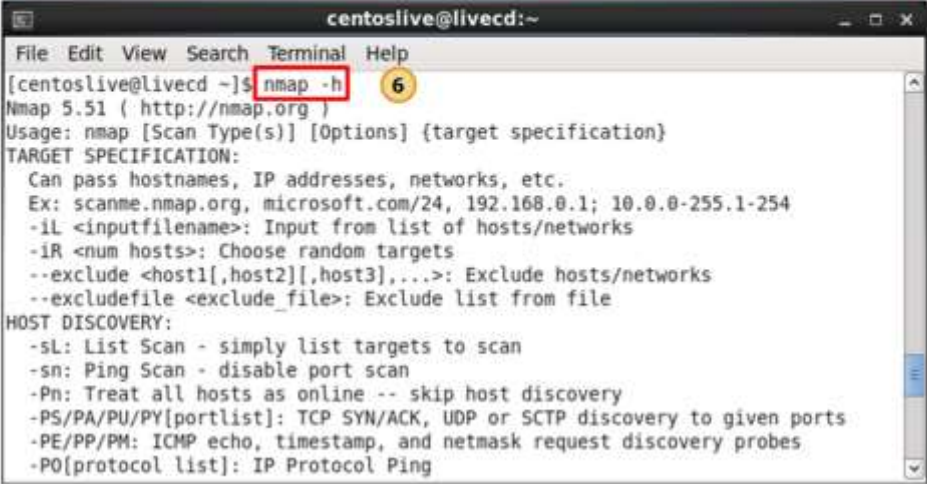


```
centoslive@livecd:~  
File Edit View Search Terminal Help  
Total download size: 2.7 M  
Installed size: 9.7 M  
Is this ok [y/N]: y  
Downloading Packages:  
nmap-5.51-3.el6.x86_64.rpm | 2.7 MB 00:17  
Running rpm_check_debug  
Running Transaction Test  
Transaction Test Succeeded  
Running Transaction  
  Installing : 2:nmap-5.51-3.el6.x86_64 1/1  
  Verifying  : 2:nmap-5.51-3.el6.x86_64 1/1  
  
Installed:  
  nmap.x86_64 2:5.51-3.el6  
  
Complete!  
[centoslive@livecd ~]$
```

### Exercise: Package Repositories (4)

This is the rest of the output from the "**yum install nmap**" command. It has now been successfully installed!

## Exercise: Package Repositories (5)



The screenshot shows a terminal window titled 'centoslive@livecd:~'. The command 'nmap -h' has been entered and executed. The output displays the Nmap 5.51 usage and target specification options. A red box highlights the command 'nmap -h', and a yellow circle with the number '6' is next to it. The terminal output is as follows:

```
centoslive@livecd:~  
File Edit View Search Terminal Help  
[centoslive@livecd ~]$ nmap -h  
Nmap 5.51 ( http://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iL <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sL: List Scan - simply list targets to scan  
  -sn: Ping Scan - disable port scan  
  -Pn: Treat all hosts as online -- skip host discovery  
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[protocol list]: IP Protocol Ping
```

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 12

### Exercise: Package Repositories (5)

6. The nmap RPM is installed. Verify you can execute nmap:

```
# nmap -h
```

You should see the usage options for nmap. This verifies that it was installed correctly.

## Exercise: Package Repositories (6)



```
centoslive@livecd:~  
File Edit View Search Terminal Help  
[centoslive@livecd ~]$ sudo yum erase nmap  
Loaded plugins: fastestmirror, refresh-packagekit, security  
Setting up Remove Process  
Resolving Dependencies  
--> Running transaction check  
---> Package nmap.x86_64 2:5.51-3.el6 will be erased  
--> Finished Dependency Resolution  
  
Dependencies Resolved  
  
=====
```

Package	Arch	Version	Repository	Size
Removing: nmap	x86_64	2:5.51-3.el6	@base	9.7 M

```
=====
```

Transaction Summary

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 13

### Exercise: Package Repositories (6)

7. Remove the nmap RPM with the "yum erase" command:

```
# yum erase nmap
```

Note how it shows you a list of exactly what actions will be performed, including any dependencies that will be affected.

## Exercise: Package Repositories (7)



```
centoslive@livecd:~  
File Edit View Search Terminal Help  
Remove      1 Package(s)  
Installed size: 9.7 M  
Is this ok [y/N]: y 8  
downloading Packages:  
Running rpm_check debug  
Running Transaction Test  
Transaction Test Succeeded  
Running Transaction  
Erasing      : 2:nmap-5.51-3.el6.x86_64      1/1  
Verifying    : 2:nmap-5.51-3.el6.x86_64      1/1  
  
Removed:  
nmap.x86_64 2:5.51-3.el6  
  
Complete!  
[centoslive@livecd ~]$
```

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 14

### Exercise: Package Repositories (7)

8. This is the rest of the output from the "**yum erase nmap**" command. Note that when you are asked if this transaction is okay, you should type "**y**".

# Review

- Which of the following commands is used to install software from an online repository?
  - install
  - yum install
  - rpm install
  - installrpm
- Which of the following commands is used to query the RPM database to determine if a package (such as tcpdump) is installed?
  - yum find tcpdump
  - rpm tcpdump
  - yum search tcpdump
  - rpm -qa | grep tcpdump

## Review

Which of the following commands is used to install software from an online repository?

install  
yum install  
rpm install  
installrpm

Which of the following commands is used to query the RPM database to determine if a package (such as tcpdump) is installed?

yum find tcpdump  
rpm tcpdump  
yum search tcpdump  
rpm -qa | grep tcpdump

# Answers

- Which of the following commands is used to install software from an online repository?
  - yum install
- Which of the following commands is used to query the RPM database to determine if a package (such as tcpdump) is installed?
  - rpm -qa | grep tcpdump
  - "rpm -qa" generates a list of all installed packages, and piping that into "grep tcpdump" searches the list for tcpdump

## Answers

Which of the following commands is used to install software from an online repository?

yum install

Which of the following commands is used to query the RPM database to determine if a package (such as tcpdump) is installed?

rpm -qa | grep tcpdump

"rpm -qa" generates a list of all installed packages, and piping that into "grep tcpdump" searches the list for tcpdump



# Software Updates

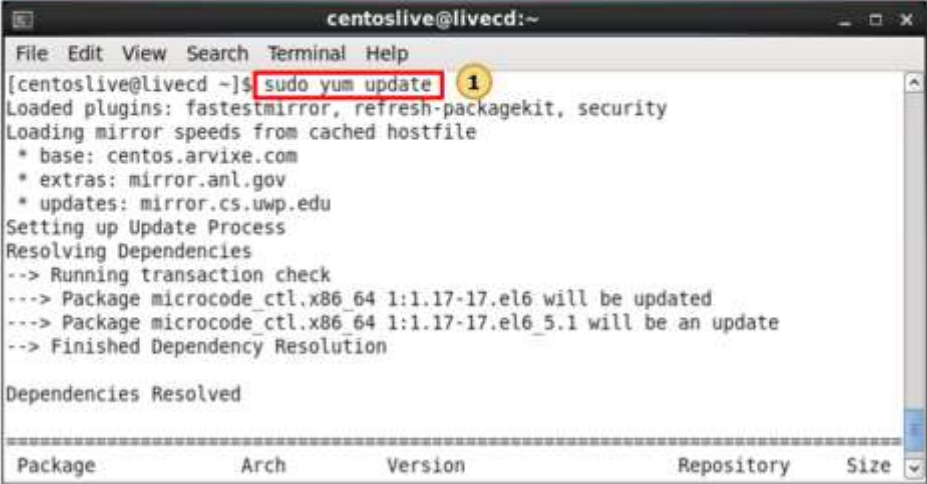
- Online repositories are particularly convenient for software updates
  - Keeping software fully patched is very important for system security!
- On Red Hat-based systems, you can update all software by running:  
`# yum update`
- To update a specific package:  
`# yum update tcpdump`
- To update all packages except a specific package:  
`# yum update --exclude tcpdump`

## Software Updates

Distribution repositories are not only handy for installing new software, but also for keeping your existing software updated. We all know that we have to keep our software updated so that we minimize our vulnerabilities and therefore reduce our risk of compromise. Keeping all of your repo software updated is as simple as running "yum update". You can also update just a specific package by specifying it's name, or leave out certain packages by using the "--exclude" option ("-x" for short). You can also use the \* as a wildcard when specifying package names. For example, the following command would update all software except anything starting with "kernel":

```
# yum update --exclude kernel*
```

# Exercise: Software Updates (1)



```
centoslive@livecd:~  
File Edit View Search Terminal Help  
[centoslive@livecd ~]$ sudo yum update 1  
Loaded plugins: fastestmirror, refresh-packagekit, security  
Loading mirror speeds from cached hostfile  
* base: centos.arvixe.com  
* extras: mirror.anl.gov  
* updates: mirror.cs.uwp.edu  
Setting up Update Process  
Resolving Dependencies  
--> Running transaction check  
--> Package microcode_ctl.x86_64 1:1.17-17.el6 will be updated  
--> Package microcode_ctl.x86_64 1:1.17-17.el6_5.1 will be an update  
--> Finished Dependency Resolution  
  
Dependencies Resolved  
  
=====
```

Package	Arch	Version	Repository	Size
---------	------	---------	------------	------

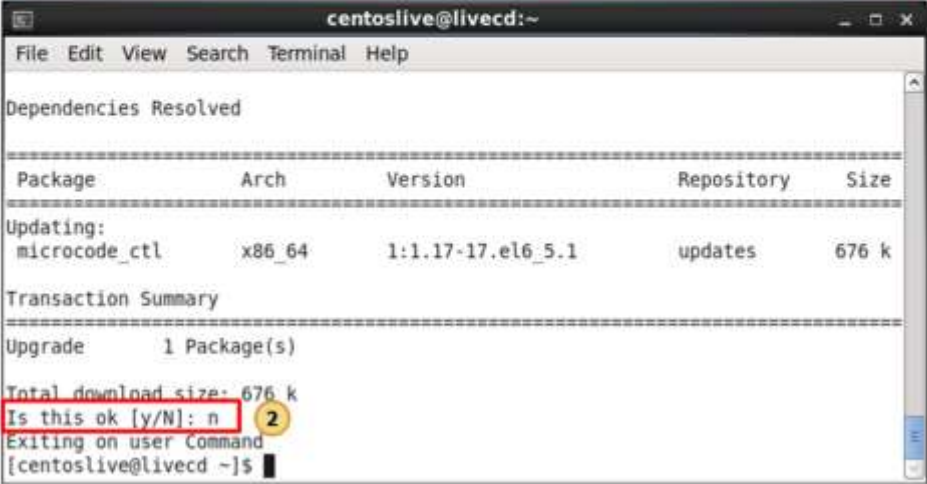
Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 18

## Exercise: Software Updates (1)

1. In your CentOS VM, open a terminal and search for updates using the command "yum update". You have to have root level access, so we prefix this command with "sudo". Note that this requires a working Internet connection.

\$ **sudo yum update**

## Exercise: Software Updates (2)



```
centoslive@livecd:~  
File Edit View Search Terminal Help  
Dependencies Resolved  


| Package                    | Arch   | Version           | Repository | Size  |
|----------------------------|--------|-------------------|------------|-------|
| Updating:<br>microcode_ctl | x86_64 | 1:1.17-17.el6_5.1 | updates    | 676 k |

  
Transaction Summary  
Upgrade      1 Package(s)  
Total download size: 676 k  
Is this ok [y/N]: n  
Exiting on user Command  
[centoslive@livecd ~]$
```

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

19

### Exercise: Software Updates (2)

2. After a few seconds, Yum will report that a certain number of packages need to be updated and ask if it's OK to continue. If this were an actual CentOS installation, we would answer "y" to continue installing the updates. However, since this is just a LiveCD environment, we don't actually want or need to install the updates. Just press Enter to accept the default answer of "No".

After you have completed this step, you can close the terminal window.

# Review Questions

- Which of the following commands is used to install software updates?
  - rpm update
  - update
  - yum update
  - installupdate
- Which of the following commands is used to update all installed RPM packages EXCEPT for httpd?
  - yum update --exclude httpd
  - yum dont-update httpd
  - yum update --without-httpd
  - yum update -httpd

# Answers

- Which of the following commands is used to install software updates?
  - `yum update`
- Which of the following commands is used to update all installed RPM packages EXCEPT for httpd?
  - `yum update --exclude httpd`

# Linux Conclusion

- This concludes our whirlwind tour of the Linux operating system
- The CentOS manuals are a great resource to learn more
- You may also wish to continue experimenting with Linux by downloading Ubuntu, Fedora, or Backtrack

## Linux Conclusion

This concludes our whirlwind tour of the Linux operating system. Once again, the CentOS manuals are very comprehensive and can be found here:

[http://www.centos.org/docs/5/html/Installation\\_Guide-en-US/](http://www.centos.org/docs/5/html/Installation_Guide-en-US/)

[http://www.centos.org/docs/5/html/Deployment\\_Guide-en-US/](http://www.centos.org/docs/5/html/Deployment_Guide-en-US/)

You may wish to continue experimenting with Linux by downloading other free distributions such as Ubuntu, Fedora, and Kali:

<http://www.ubuntu.com/>

<http://fedoraproject.org/>

<http://www.kali.org/>